

(19)日本国特許庁(J P)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平5-151091

(43)公開日 平成5年(1993)6月18日

(51)Int.Cl.⁵G 0 6 F 12/14
1/00
12/14

識別記号

3 2 0 A 9293-5B
3 7 0 E 7927-5B
3 2 0 D 9293-5B

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数25(全 18 頁)

(21)出願番号 特願平3-312233

(22)出願日 平成3年(1991)11月27日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72)発明者 園部 正幸

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(74)代理人 弁理士 竹内 進 (外1名)

(54)【発明の名称】 情報処理装置の機密情報管理方式

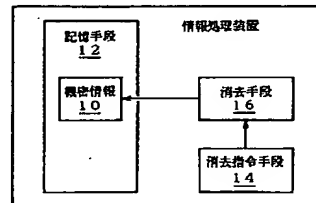
(57)【要約】

【目的】記憶装置に格納された機密情報が本人以外の第三者により利用されることを防止する情報処理装置の機密情報管理方式に関し、携帯時や長時間の離席に際して本人以外の者による機密情報の利用を簡単な操作で確実に防止することを目的とする。

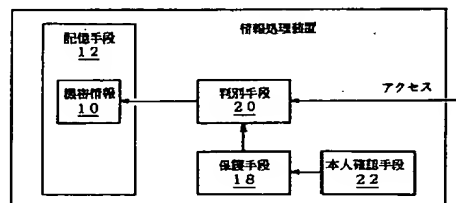
【構成】記憶手段12に格納した機密情報10の消去を消去指令手段14で指令した際に、消去手段16が記憶手段12の機密情報10を消去する。例えば利用者のスイッチ操作時に自動的に機密情報10を消去する。スイッチ操作等で機密情報10のアクセス禁止を設定する保護手段18を設け、判別手段20でアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。アクセス禁止の設定解除は本人確認手段22で行う。

本発明の原理説明図

(a)



(b)



1

【特許請求の範囲】

【請求項1】機密情報10を格納した記憶手段12と、前記機密情報10の消去を指令する消去指令手段14と、該消去指令手段14の消去指令出力に基づいて前記記憶手段12に格納された機密情報10を消去する消去手段16とを備えたことを特徴とする情報処理装置の機密情報管理方式。

【請求項2】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は操作スイッチを備え、利用者のスイッチ操作時に自動的に機密情報10を消去することを特徴とする情報処理装置の機密情報管理方式。

【請求項3】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時に自動的に機密情報10を消去することを特徴とする情報処理装置の機密情報管理方式。

【請求項4】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、外部からの電源供給の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項5】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、外部の電話線との接続断を電話線の電気状態から判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項6】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、外部の電話線の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項7】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、外部のモデムとの接続断をモデムとの間の電気状態で判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項8】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、外部のモデムの接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項9】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項10】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、パケット

2

組立分解装置の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項11】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、ICカードが抜かれたことを電気状態で判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項12】請求項1記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段14は、ICカードが抜かれたことを接続部が外れたことで判別した時に消去指令を出力して自動的に機密情報10を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項13】機密情報10を格納した記憶手段12と、前記機密情報10のアクセス禁止を設定する保護手段18と、機密情報10のアクセスを受けて際に前記保護手段18がアクセス禁止を設定していれば機密情報10のアクセスを禁止し、アクセス禁止を解除していれば機密情報のアクセスを許可する判別手段20と、利用者本人を確認して前記保護手段18のアクセス禁止を設定解除する本人確認手段22とを備えたことを特徴とする情報処理装置の機密情報管理方式。

【請求項14】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は操作スイッチを備え、利用者のスイッチ操作時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項15】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項16】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、外部からの電源供給の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項17】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、外部の電話線との接続断を電話線の電気状態から判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項18】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、外部の電話線の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状

態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項19】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段16は、外部のモデムとの接続断をモデムとの間の電気状態で判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項20】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、外部のモデムの接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項21】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項22】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、パケット組立分解装置の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項23】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、ICカードが抜かれたことを電気状態で判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項24】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記保護手段18は、ICカードが抜かれたことを接続部が外れたことで判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項25】請求項13記載の情報処理装置の機密情報管理方式に於いて、前記本人確認手段22は、利用者が暗証コードを入力した時或いは装置の鍵を解錠した時に前記保護手段18のアクセス禁止を設定解除して機密情報の読み書きを可能とする非保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、記憶装置に格納された機密情報が本人以外の第三者により利用されることを防止する情報処理装置の機密情報管理方式に関する。

【0002】

【従来の技術】近年、携帯の容易な情報処理装置としてパーソナルコンピュータ、ワードプロセッサ、電子手帳等が広く普及している。こうした情報処理装置は、個人で利用されることが多く、更には企業機密にかかわるビジネスにも利用されており、情報処理装置に格納された機密情報の保護がプライバシーや企業秘密を守るために強く求められている。

【0003】ここで機密情報の保護は、機密情報の読出し、書込み、または実行について考えられ、これらを総称して、アクセス (access) という。また、近年は会員制のパーソナルコンピュータの通信システムも広範に普及しており、システムの利用料金は持ち主に請求されるが、持ち主しか知らないID (利用者識別番号) やパスワード (暗証コード) を記憶装置に内蔵している機器においては、万一盗まれた場合、持ち主になりますまして使われてしまい、料金だけが持ち主に請求されるという問題が生じる。

【0004】また、ファイルやデータベースを暗号化したときの暗号化鍵コードを知られると、ファイルやデータベースの中の機密情報にアクセスできてしまう。更に、さまざまな知人や会社等の機密情報が、記憶装置に内蔵されていたり、あるいは、盗まれた情報処理装置に持ち主の通信用のパスワードが含まれていて犯人に漏れた場合、機密情報の中にまた別の機密情報のパスワードが格納されている場合があり、機密情報がいったん漏洩すると、影響はどんどん拡大する。

【0005】従って、情報処理装置を家庭やオフィスで使っているときには、機密情報を持ち主本人が自由に使えるほうがよいが、情報処理装置を外へ持出すときとか、席を外すときには、万一盗まれてもよいように、他人が機密情報に触れることを不可能な状態に簡単に切替えるということが要請される。従来の情報処理装置の機密保護にあつては、機密情報、情報サービス、動作或いは表示を暗証コードの入力で保護し、電源オンから暗証コード入力して不揮発性メモリに内蔵した正解の暗証コードと一致するまでは、機密情報、情報サービス、動作或いは表示をさせないといった技術が採用されている。

【0006】

【発明が解決しようとする課題】しかしながら、暗証コードを入力するようにした従来の機密情報保護方式にあつては、機密情報を消去、或いは暗証コードまたは鍵を開けないと機密情報にアクセスできないように保護をかけることを管理ソフトウェアに命ずる操作が繁雑であり、使い難いために保護機能が有効に活用されない問題があつた。

【0007】また従来より記憶装置の全部の内容を消去するスイッチを設けた機器もあり、操作は簡単であるが、これでは保護を必要としない多くの情報が一緒に消去されてしまう不都合があつた。更に、暗証コードの入力により起動するタイマを設け、タイマの設定時間が経

過するまでは機密情報のアクセスを許可し、タイマの設定時間を超えると、再度暗証コードを入力しなければ機密情報の読み書き実行が不可能な保護状態に切替わる機密情報管理方式もある。

【0008】しかし、タイマを用いた従来方式は、設定時間を短くすると、次に機密情報をアクセスする前に保護状態に切替わってしまうために頻繁に暗証コードの入力を必要とし、一方、タイマの設定時間を長くすると、席を外した時等に他人により機密情報が使われてしまう可能性が大きくなるという問題があった。本発明は、このような従来の問題点に鑑みてなされたもので、携帯時や長時間の離席に際して本人以外の者による機密情報の利用を簡単な操作で確実に防止できるようにした情報処理装置の機密情報管理方式を提供することを目的とする。

【0009】

【課題を解決するための手段】図1は本発明の原理説明図である。まず本発明による情報処理装置の機密情報管理方式は、図1(a)に示すように、機密情報10を格納した記憶手段12と、機密情報10の消去を指令する消去指令手段14と、消去指令手段14の消去指令出力に基づいて記憶手段12に格納された機密情報10を消去する消去手段16とを備えたことを特徴とする。

【0010】ここで消去指令手段14は次の(1)～(10)の形態をとる。

(1) 操作スイッチを備え、利用者のスイッチ操作時に自動的に機密情報10を消去する。

(2) 装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時に自動的に機密情報10を消去する。

【0011】(3) 外部からの電源供給の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させる。

(4) 外部の電話線との接続断を電話線の電気状態から判別した時に消去指令を出力して自動的に機密情報10を消去させる。

(5) 外部の電話線の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させる。

【0012】(6) 外部のモデムとの接続断をモデムとの間の電気状態で判別した時に消去指令を出力して自動的に機密情報10を消去させる。

(7) 外部のモデムの接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報10を消去させる。

(8) パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時に消去指令を出力して自動的に機密情報10を消去させる。

【0013】(9) パケット組立分解装置の接続部が外れたことを判別した時に消去指令を出力して自動的に機

密情報10を消去させる。

(10) ICカードが抜かれたことを電気状態で判別した時に消去指令を出力して自動的に機密情報10を消去させる。

(11) ICカードが抜かれたことを接続部が外れたことで判別した時に消去指令を出力して自動的に機密情報10を消去させる。

【0014】また本発明による情報処理装置の機密情報管理方式は図1(b)に示すように、機密情報10を格納した記憶手段12と、機密情報10のアクセス禁止を設定する保護手段18と、機密情報10のアクセスを受けて際に前記保護手段18がアクセス禁止を設定していれば機密情報10のアクセスを禁止し、アクセス禁止を解除していれば機密情報のアクセスを許可する判別手段20と、利用者本人を確認して前記保護手段18のアクセス禁止を設定解除する本人確認手段22とをを備えたことを特徴とする。

【0015】ここで保護手段18は次の(1)～(11)の形態をとる。

(1) 操作スイッチを備え、利用者のスイッチ操作時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

(2) 装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

【0016】(3) 外部からの電源供給の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

(4) 外部の電話線との接続断を電話線の電気状態から判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

(5) 外部の電話線の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

【0017】(6) 外部のモデムとの接続断をモデムとの間の電気状態で判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

(7) 外部のモデムの接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

【0018】(8) パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

(9) パケット組立分解装置の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

【0019】(10) ICカードが抜かれたことを電気

状態で判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

(11) ICカードが抜かれたことを接続部が外れたことで判別した時にアクセス禁止を設定して機密情報10の読み書きを不可能とする保護状態に切替える。

【0020】更に図1(b)の本人確認手段22は、利用者が暗証コードを入力した時或いは装置の鍵を解錠した時に保護手段18のアクセス禁止を設定解除して機密情報の読み書きを可能とする非保護状態に切替える。

【0021】

【作用】このような構成を備えた本発明の情報処理装置の機密情報管理方式によれば、携帯や長時間離席に際してスイッチ操作、AC電源線の外し、外部通信回線と接続外し等を行うと、自動的に機密情報の消去や保護状態の設定が自動的に行われ、操作がきわめて容易か特別な操作を必要とせず、機密情報の保護を確実に行うことができる。

【0022】これにより、万が一、情報処理装置が盗難にあっても、盗難時の電源外しや通信回線の外しで機密情報が自動消去されたりアクセス不可能な保護状態に自動的に切替わり、その後の機密情報の利用を不可能にして悪用を未然に防止できる。

【0023】

【実施例】図2は本発明の第1実施例の基本構成を示した実施例構成図である。図2において、24は情報処理装置であり、例えばパーソナルコンピュータ、ワードプロセッサ、電子手帳等である。尚、以下の実施例にあっては情報処理装置24としてパーソナルコンピュータを例にとって説明する。

【0024】情報処理装置24には記憶装置12が設けられ、記憶装置12の特定の記憶領域には機密情報10が格納されている。また、情報処理装置24には記憶装置12の書込み、読出し、更には命令の実行を行う制御装置26が設けられる。制御装置26に対してはキーボードやマウス等により利用者からの操作入力を与えられ、この操作入力に基づくコマンドを実行する。

【0025】本発明の機密情報管理方式にあっては、消去指令手段としてのスイッチ14と消去部16を新たに設けている。スイッチ14は例えば情報処理装置24のケースに設けられた操作スイッチであり、スイッチ14をオン操作すると消去部16に対し機密情報の消去指令が与えられる。消去部16はスイッチ14のオン操作による消去指令を受けると記憶装置12に格納している機密情報10を強制的に消去する処理を行う。

【0026】図3は図2の情報処理装置24に設けた消去部16の処理動作を示したフローチャートである。図3において、まずステップS1で消去部16はスイッチ14のオン、オフを監視しており、スイッチ14がオンされるとステップS2に進み、記憶装置12の機密情報10を強制的に消去する。

【0027】具体的な使い方としては、例えば家庭や会社に情報処理装置を置いた通常の利用状態では情報処理装置24をパワーオンスタートした動作状態であれば自由に記憶装置12の機密情報10を機密情報10以外の記憶情報と同様、制御装置26からアクセスすることができる。一方、利用者が情報処理装置24を例えば携帯して外出する場合や、あるいは電源を投入したまま長時間席を離れるような場合にはスイッチ14を閉じる。スイッチ14を閉じると、図3のフローチャートに示したように消去部16が自動的に記憶装置12内の機密情報10を消去する。従って、その後第三者が情報処理装置24を操作しても記憶装置12内の機密10は無くなっているため機密情報10のアクセスは不可能となり、プライバシー情報やIDカード等の機密情報が第三者に知られてしまうことを確実に防止できる。

【0028】更に、利用者が再び情報処理装置24を使用する際に、もし機密情報10が必要となれば再度自分で機密情報10を記憶装置12に入力するか外部システムの記憶装置と通信接続した情報入力により機密情報10を作ることになる。図4は図2の実施例を具体化したラップトップ型のパーソナルコンピュータの説明図であり、図5に側面図を示す。

【0029】図4において、ラップトップ型のパーソナルコンピュータとしての情報処理装置はキーボード28を備えた計算機本体30と、計算機本体30に対し開閉自在なカバー部32で構成され、カバー部32の内側には液晶ディスプレイ34が設けられている。計算機本体30の右側面にはICカード36が挿入されている。また、図5の側面図から明らかなように、計算機本体30の後部側にメインスイッチ38が設けられ、更にDCコネクタ40を設けている。このDCコネクタ40に対しては、後の説明で明らかにするようにACアダプタの出力端子が接続され、DCコネクタ40にACアダプタの出力端子が接続されると自動的に計算機本体30はそれまでのバッテリーモードから商用交流電源を使用して動作するACモードに切り換わる。

【0030】更に、計算機本体30内には小型磁気ディスク装置としてハードディスク(HDD)が格納されている。図4のパーソナルコンピュータにおいて、図2の実施例に示したスイッチ14は計算機本体30の前部右端に設けられており、スイッチ14を消去位置に操作することで計算機本体30内の記憶装置12、例えばRAMに格納されている機密情報10を自動的に消去することができる。

【0031】図6は図4、図5に示したラップトップ型パーソナルコンピュータにおける計算機本体30の一実施例を示した実施例構成図である。図6において、計算機本体30にはCPU42が設けられ、CPU42からは内部バス44が引き出される。CPU42に対しては制御プログラムを格納したROM46と一時的にデータ

を記憶保持するRAM48が設けられる。本発明にあっては、RAM48の中に機密情報10を格納している。

【0032】また、ディスプレイコントローラ50を介して液晶ディスプレイ34が設けられ、ディスプレイコントローラ50はビデオRAM52に格納された画像データを表示する。このビデオRAM52に格納された画像データについても、RAM48と同様、特定の情報を機密情報10として扱うようにしてもよい。更にキーボードコントローラ54を介してキーボード28が接続される。

【0033】内部バス44の右側にはICカードコントローラ56とその入出力を行う入出力インタフェース58及びICカードアダプタ60が設けられる。ICカードアダプタ60に対しては外部よりICカード36を着脱することができる。また、内部バス44の右側にはディスクコントローラ62との入出力インタフェース64及び小型磁気ディスクを用いたハードディスク66が設けられている。このハードディスク66の出力情報についてもRAM48と同様、特定の情報について機密情報10として格納することができる。

【0034】また、内部バス44の右側にはプリントコントローラ68との入出力インタフェース70が設けられ、外部にプリンタ装置72を接続することができる。更に、内部バス44の右側には通信コントローラ74との入出力インタフェース76が設けられ、外部のモデム(変復調装置)78を介して電話回線等の通信回線80を接続することができる。

【0035】これに加えて本発明の機密情報管理方式にあっては、内部バス44に対し消去部16が設けられ、消去部16にはスイッチ14が接続されている。消去部16はスイッチ14のオン操作による消去指令を受けた際に、例えば割込みをCPU42に対し発行し、CPU42の制御のもとにRAM48に格納されている機密情報10の消去処理を行う。

【0036】更に計算機本体30には電源回路82とバッテリー84が設けられている。電源回路82にはDCコネクタ40が接続され、DCコネクタ40に対してはACアダプタ86の出力端子としてのプラグ88が接続される。会社や家庭等において使用する際には、通常、ACアダプタ86のプラグ88がDCコネクタ40に接続され、ACアダプタ86は商用AC100Vを受けて規定の直流電圧に整流平滑して電源回路82に供給し、電源回路82は各回路部に規定の電源電圧を供給する。

【0037】一方、外出先等で使用する際には商用電源を取ることができないため、DCコネクタ40からACアダプタ86のプラグ88は外されており、この状態ではバッテリー84から電源回路82に電源供給が行われる。尚、ACアダプタ86の使用時には、電源回路82を介してバッテリー84の充電が同時に行われる。図7は図2に示したスイッチ14のラップトップ型パーソナ

ルコンピュータにおける他の実施例を示した説明図である。

【0038】図7の実施例にあっては、計算機本体30のキーボード28の設置面の左上隅にスイッチ14を設け、このスイッチ14に相対するカバー部32の内側に突起90を設けている。スイッチ14は図示のカバー部32を開放した状態では、図示のように突出して例えばスイッチオフ状態にあり、図2に示した消去部16に対する消去指令の出力を禁止している。

【0039】一方、外出時や席を離れる際にカバー部32を閉じると、カバー部32の内側に設けた突起90が計算機本体90側のスイッチ14を押圧してスイッチ14がオンし、これにより記憶装置の機密情報10の消去が自動的に行われる。この図7の実施例にあっては、機密情報を消去するための特別な操作は必要とせず、カバー部32を閉じることによって自動的に機密情報の消去ができる。

【0040】図8は本発明の消去指令手段の他の実施例を示した実施例構成図であり、この実施例にあっては、ACアダプタ86のプラグ88をDCコネクタ40から抜いたことを判別して機密情報を自動的に消去するようにしたことを特徴とする。図8は装置本体側のDCコネクタ40にACアダプタのプラグ88を差し込んだ状態を示す。

【0041】プラグ88は中央先端に突出した電極部92と絶縁部94を介して背後に設けた電極部96を有し、この実施例にあっては、電極部92がマイナス側、電極部96がプラス側となっている。DCコネクタ40は中央先端の電極部92に接触する接点部材98と電極部96に接触する外側の接点部材100を備える。接点部材98は内部のマイナスライン102に接続され、また接点部材100は内部のプラスライン104に接続される。プラスライン104とマイナスライン102の間にバッテリー84が接続される。このうちプラスライン104からは抵抗106とダイオード108の充電回路を介してバッテリー84のプラス側が接続される。

【0042】バッテリーのプラス側はDCコネクタ40のスイッチ部材110に接続される。スイッチ部材110は図示のようにプラグ88を差し込んだときの接点部材100の外側への変形部でプラスライン104との接続が切り話されている。更に、DCコネクタ40にはスイッチ部材112が設けられる。スイッチ部材112はスイッチ部材110とは逆にプラグ88を差し込むと図示のようにプラスライン104に接続される。

【0043】バッテリー84の出力側には図2の消去部16に対し消去指令信号を出力するためのフリップフロップ114が接続され、フリップフロップ114の入力にはDCコネクタ40のスイッチ部材112が接続される。116は入力用の抵抗である。図8のプラグ88を差し込んだ状態にあっては、ACアダプタで整流された

直流電圧がDCコネクタ40を介してプラスライン104及びマイナスライン102により直接装置の電源回路に供給されている。このときスイッチ部材110は接点部材110から離れており、従ってバッテリー84はプラスライン104より抵抗106及びダイオード108を介して充電電流を受ける。

【0044】一方、スイッチ部材112が接点部材100に接触していることからフリップフロップ114にHレベル入力が行われ、フリップフロップ114はセット状態となることで消去部16に対し消去指令信号の出力を停止している。図9は図8のプラグ88をDCコネクタ40から抜いた状態を示す。プラグ88をDCコネクタ40から抜くと、接点部材98及び100は変形状態から元の水平な状態に戻る。このため、接点部材100に対するスイッチ部材112の接触が断たれ、同時にスイッチ部材110が接点部材100に接触する。

【0045】これによって、バッテリー84からのプラス電圧がスイッチ部材110、接点部材100を介してプラスライン104に供給され、バッテリー84による電源供給状態に切り換わる。同時にスイッチ接点112が離れることでフリップフロップ114に対する入力がLレベルに立ち下がり、フリップフロップ114がリセットされることで消去部16に対し消去指令信号を出力し、プラグ88を抜くと自動的に機密情報の消去が行われる。

【0046】尚、図8、図9の実施例ではプラグ88を書き込んだときにフリップフロップ114をセットしプラグ88を抜いたときにフリップフロップ114をリセットしているが、逆にプラグ88の差し込みでフリップフロップ114をリセットしプラグ88を抜くことでフリップフロップ114をセットするようにしてもよい。

【0047】このような図8、図9に示す外部から電源供給の接続部が外れたことを判別して機密情報を自動的に消去できるようにすることで、家庭や会社で使用している場合には通常、ACアダプタを接続して外部から電源供給しているが、外出時には当然にACアダプタを外すことから、外部からの電源供給の接続が外れることで自動的に機密情報の消去が行われる。また、席を長時間離れるような場合にもACアダプタを外しておけば、同様に機密情報が消去できる。

【0048】図10は本発明の消去指令手段の他の実施例をラップトップ型パーソナルコンピュータの計算機本体30について示した実施例構成図である。この図10の実施例にあつては、消去部16に対する消去指令を監視部116より出力するようにしたことを特徴とする。監視部116はこの実施例にあつては、ICカードアダプタ60に対するICカード36の着脱状態、通信回線80を接続したモデム78の状態、更に電源回路82に対する外部からの電源供給状態を監視している。

【0049】監視部116の具体的な実施例としては、

次の ～ がある。

外部からの電源回路82に対する電源供給の接続部が外れたことを判別して消去部16に対し消去指令信号を出力する。

モデム78に通信回線80として電話回線を接続している場合、電話回線の接続断を電話回線の電気状態で判別して消去部16に消去指令信号を出力する。

【0050】と同様、通信回線80として電話回線を接続している場合、電話回線の接続部、例えばモジュージャック等が外れたことを判別して消去部16に消去指令信号を出力する。

モデム78との接続断をモデム78との電気状態、例えばキャリア有無で判別し、キャリア無しを判別したときに消去部16に対し消去指令信号を出力する。

【0051】モデム78と接続しているケーブル接続部が外れたことを判別して消去部16に消去指令信号を出力する。

通信回線80によりパケット通信を行う場合に、モデム78に内蔵されたパケット組立分解装置(PADパケットアッセンブリ・リアッセンブリ装置)との接続断をパケット組立分解装置との間の電気状態で判別して消去部16に消去指令信号を出力する。

【0052】モデム78に設けたパケット組立分解装置のケーブル接続が外れたことを判別して消去部16に消去指令信号を出力する。

ICカードアダプタ60からICカード36が抜かれたことを電気状態で判別して消去部16に消去指令信号を出力する。

ICカードアダプタ60からICカード36が抜かれたことをICカード36とICカードアダプタ60の接続部が外れたことで判別して消去部16に消去指令信号を出力する。

【0053】図11は本発明の第2実施例の基本構成を示した実施例構成図である。図11において、情報処理装置24には機密情報10を格納した記憶装置12が設けられ、制御装置26により外部からの指令に基づいて機密情報10を含む記憶情報のアクセスが行われる。機密情報10を保護するため、この実施例にあつては保護部18を構成するセット回路部120と保護フリップフロップ124、制御装置26の1つの機能として設けられる判別部20、更に保護フリップフロップ124のリセットを行う本人確認部22が設けられる。セット回路部120はスイッチ14のオン、オフに基づいて保護フリップフロップ124に対するセット動作を行う。

【0054】情報処理装置24の電源を投入してパワーオンスタートさせた状態にあつては保護フリップフロップ124はリセット状態にあり、判別部20に対し非保護を指令している。このため、制御装置26は記憶装置12の機密情報10をアクセスすることができる。一方、スイッチ14をオンするとセット回路部120が保

13

保護フリップフロップ 124 をセットして保護状態に設定する。この保護状態にあっては、制御装置 26 の判別部 20 がアクセスを受けた際に保護フリップフロップ 124 の保護状態を判別し、もし機密情報 10 に対するアクセスであれば、このアクセスを禁止する。

【0055】従って、外出の際や長時間席を離れる際にスイッチ 14 を操作しておけば自動的に機密情報 10 に対する制御装置 26 からの読み書きを不可能とする保護状態に切り換えることができる。一度セット状態となった保護フリップフロップ 124 は本人確認部 22 における本人確認に基づいてリセットされ、非保護状態とすることができる。本人確認部 22 における本人確認の手法としては、電磁気的紙の操作、ID カードや IC カードの差し込み等の公知の方法を用いることができる。

【0056】尚、上記の実施例では、電源投入をしたパワーオンスタート時に保護フリップフロップ 124 を最初リセット状態としているが、保護を確実にするためには、パワーオンスタート時に保護フリップフロップ 124 をセット状態とし、本人確認部 22 に対する確認処理を行って初めて保護フリップフロップ 124 をリセットして非保護とできるようにすることができる。このようにすれば、本人確認部 22 による本人確認を一度行えばスイッチ 14 をオンするまでは何回でも機密情報 10 をアクセスすることができる。

【0057】図 12 は図 11 の制御装置 26 に設けた判別部 20 による機密保護処理を示したフローチャートである。図 12 において、まず装置をパワーオンスタートするとステップ S1 で機密情報のアクセスの有無を監視しており、機密情報のアクセスでなければステップ S3 に進んでアクセスを許可する。一方、機密情報のアクセスであった場合にはステップ S2 で保護フリップフロップ 124 がセット状態かどうかチェックする。セット状態になれば非保護であることからステップ S3 に進んでアクセスを許可する。セット状態であれば保護であることからステップ S4 に進み、機密情報のアクセスを禁止する。

【0058】図 13 は図 11 の実施例をラップトップ型パーソナルコンピュータに適用した場合の計算機本体 30 の実施例構成図である。この図 13 の実施例にあっては、CPU 42 からの内部バス 44 に対し保護フリップフロップ 124 の出力を供給し、保護フリップフロップ 124 はスイッチ 14 を備えたセット回路部 120 によりリセットできるようにしている。また、保護フリップフロップ 124 のリセットは IC カード 36 の挿入等による CPU 42 による本人確認の処理結果を内部バス 44 より受けてリセットする。

【0059】それ以外の計算機本体 30 の構成は図 6 の実施例と同じである。また図 13 の実施例におけるスイッチ 14 としては、図 4 の計算機本体 30 の前部に設けたスイッチ 14、図 7 の計算機本体 30 のキーボード面

14

の隅に設けたスイッチ 14 とカバー部 32 の突起 90 により蓋を閉じることでオンするスイッチ、更に図 8、図 9 に示した AC アダプタのプラグ 88 の DC コネクタ 40 に対する着脱を検出する実施例のいずれかをそのまま適用することができる。

【0060】尚、図 8、図 9 の実施例にあっては、フリップフロップ 114 を図 13 の保護フリップフロップ 124 としてもよい。更に図 13 の実施例についても、図 10 の実施例と同様、スイッチ 14 の代わりに監視部 116 を設け、図 10 について前述した ~ のいずれかの状態を判別したときにセット回路部 120 よりセット信号を保護フリップフロップ 124 に出力して保護フリップフロップを保護状態に設定し、機密情報 10 のアクセスを禁止させるようにしてもよい。

【0061】更に上記の実施例は機密情報の自動消去とアクセスを禁止する保護モードへの切替えを例にとるものであったが、情報処理装置に消去機能と保護機能の 2 つを設け、暗証コード等の入力で機密情報の自動消去モードと保護モードとを切替えできるようにしてもよい。更に、上記の実施例はラップトップ型パーソナルコンピュータを例にとるものであったが、本発明はこれに限定されず、個人的に使用されるワードプロセッサや電子手帳等の適宜の情報処理装置にそのまま適用することができる。

【0062】

【発明の効果】以上説明してきたように本発明によれば、情報処理装置を携帯する場合や長時間席を離れる場合に機密情報を消去するかあるいは機密情報のアクセスを禁止する保護状態を簡単な操作あるいは特別な操作を必要とすることなく実現でき、第三者に機密情報が見られたり盗難時に機密情報が知られて悪用されてしまう等の問題を未然に防ぎ、情報処理装置の小形化に伴う機密保護の強い要求に適切に対応することができる。

【図面の簡単な説明】

【図 1】本発明の原理説明図

【図 2】本発明の基本的な第 1 実施例を示した実施例構成図

【図 3】図 2 の実施例による機密情報の消去処理を示したフローチャート

【図 4】図 2 の実施例を適用したパーソナルコンピュータの説明図

【図 5】図 4 の側面図

【図 6】図 4 の計算機本体の実施例構成図

【図 7】蓋の開鎖でスイッチを作動して機密情報を消去させるパーソナルコンピュータの説明図

【図 8】AC アダプタのプラグ抜きを検出して機密情報を消去させる回路のプラグ装着状態の実施例構成図

【図 9】図 8 についてプラグを抜いた状態を示した実施例構成図

【図 10】監視部により機密情報の消去条件を判別する

ようにした計算機本体の他の実施例構成図

【図11】本発明の基本的な第2実施例を示した実施例構成図

【図12】図10の実施例による機密情報の保護処理を示したフローチャート

【図13】図11の実施例を適用したマイクロコンピュータ計算機本体の実施例構成図

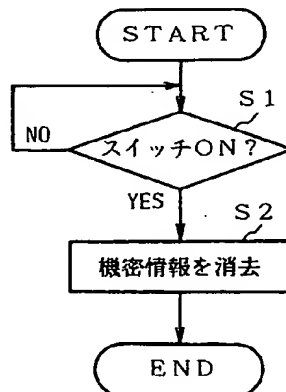
【符号の説明】

10：機密情報
12：記憶手段
14：消去指令手段（スイッチ）
16：消去手段（消去部）
18：保護手段（保護部）
20：判別手段（判別部）
22：本人確認手段（本人確認部）
24：情報処理装置
26：制御装置
28：キーボード
30：計算機本体
32：カバー部
34：液晶ディスプレイ
36：ICカード
38：メインスイッチ
40：DCコネクタ
42：CPU
44：内部バス
46：ROM
48：RAM
50：ディスプレイコントローラ

52：ビデオRAM
54：キーボードコントローラ
56：ICカードコントローラ
58, 64, 70, 76：入出力インタフェース
60：ICカードアダプタ
62：ディスクコントローラ
66：ハードディスク
68：プリンタコントローラ
72：プリンタ装置
74：通信コントローラ
78：モデム
80：通信回線
82：電源回路
84：バッテリー
86：ACアダプタ
88：プラグ
90：突起
92, 96：電極
94：絶縁部
98, 100：接触部材
102：マイナスライン
104：プラスライン
106, 116：抵抗
108：ダイオード
110, 112：スイッチ部材
114：フリップフロップ（FF）
116：監視部
120：セット回路部
124：保護フリップフロップ

【図3】

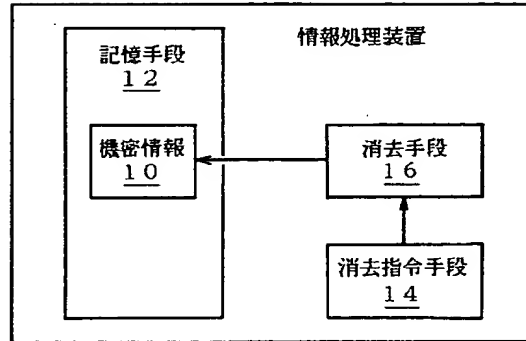
図2の実施例による機密情報の消去処理を示したフローチャート



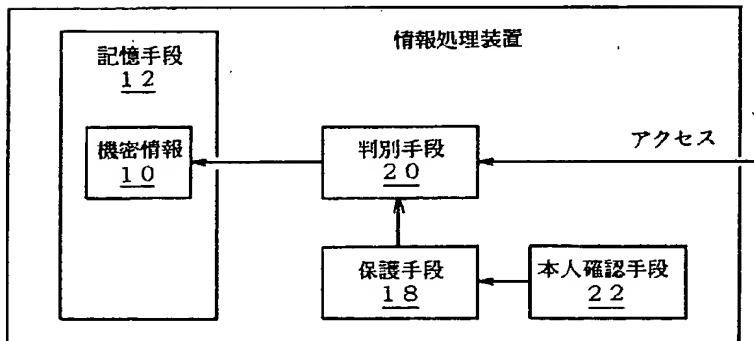
【図 1】

本発明の原理説明図

(a)

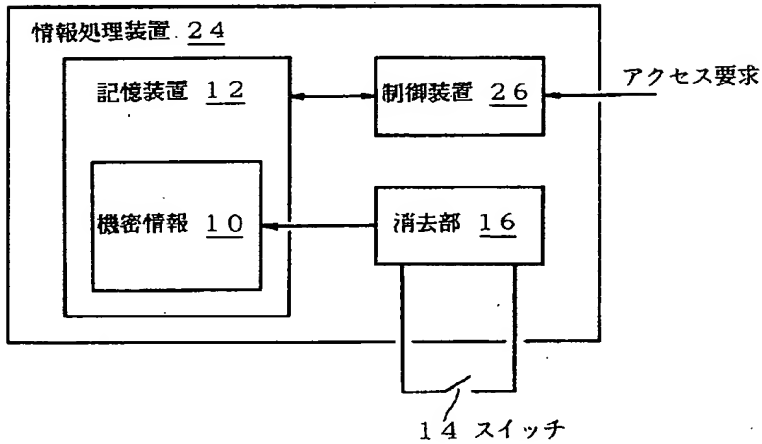


(b)



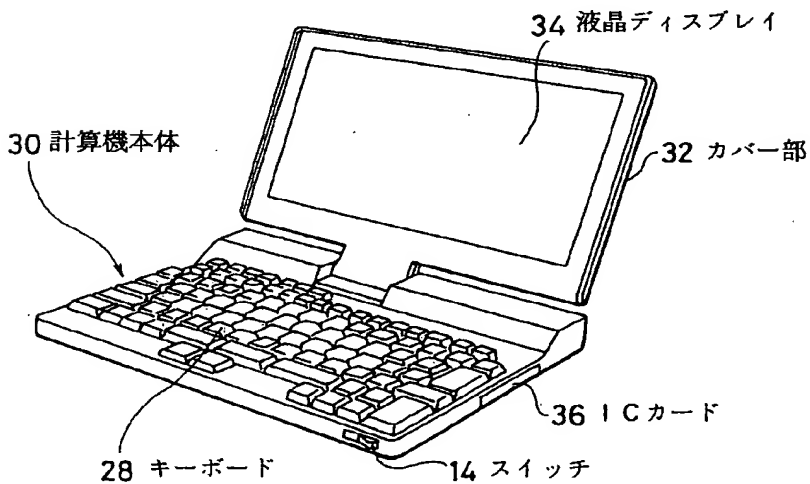
【図2】

本発明の基本的な第1実施例を示した実施例構成図



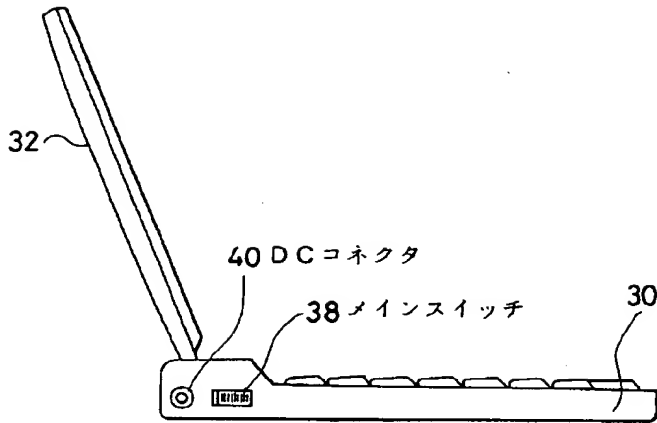
【図4】

図2の実施例を適用したパーソナルコンピュータの説明図



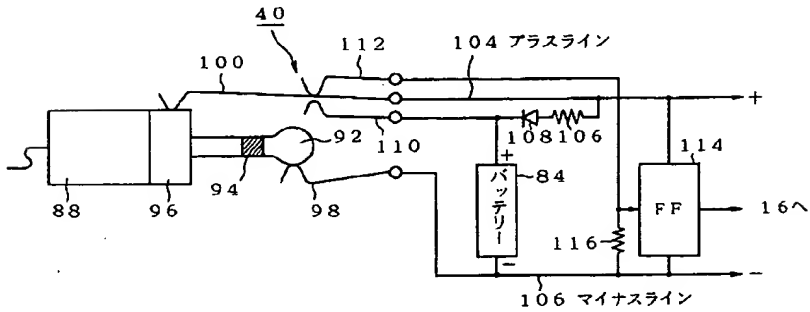
【図5】

図4の側面図



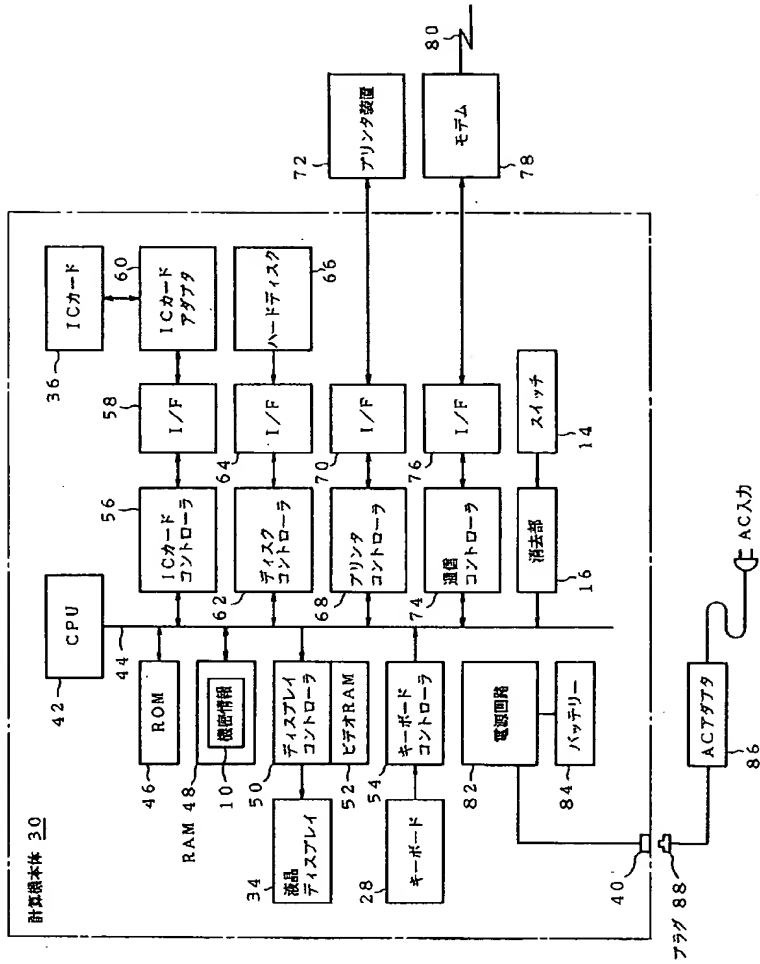
【図8】

ACアダプタのプラグ抜きを検出して機密情報を消去させる回路のプラグ装着状態の実施例構成図



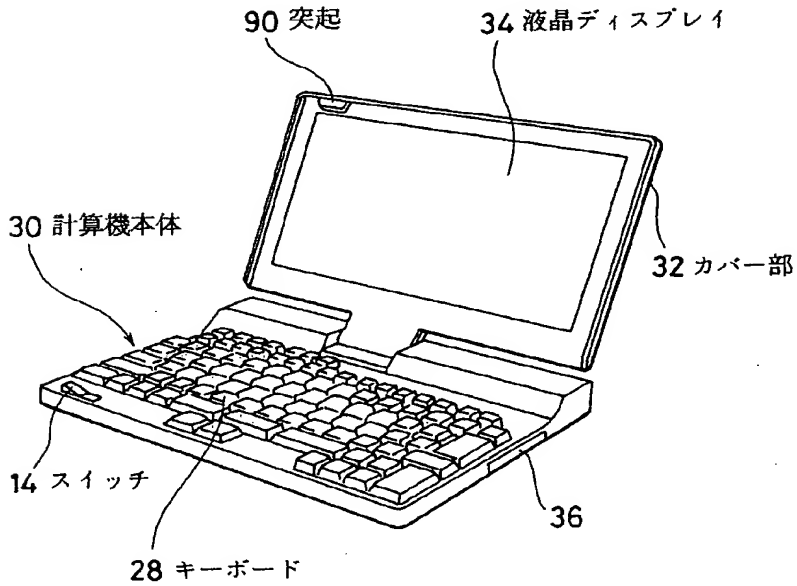
【図6】

図4の計算機本体の更詳細構成図



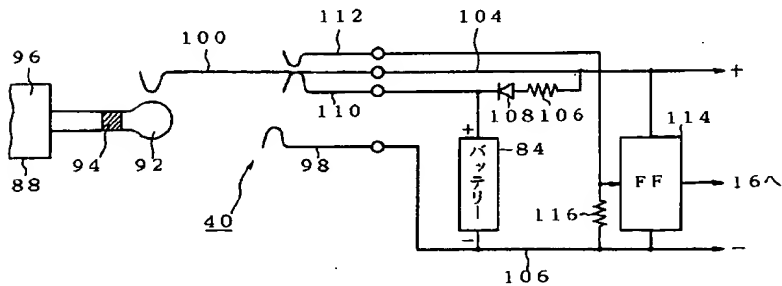
【図7】

蓋の開鎖でスイッチを作動して機密情報を消去させる
パーソナルコンピュータの説明図



【図9】

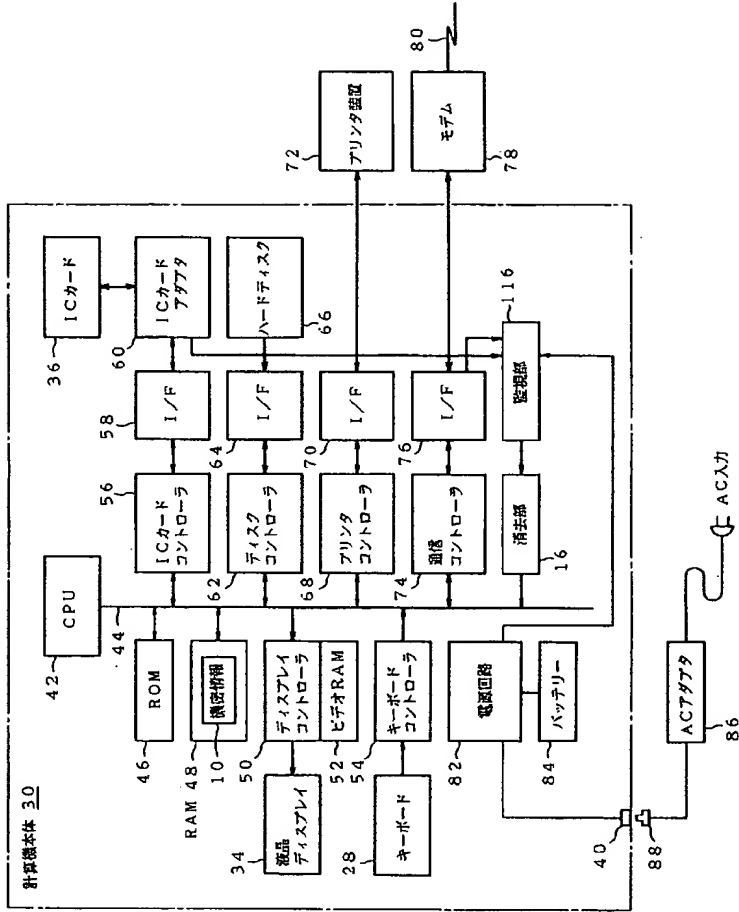
図8についてプラグを抜いた状態を示した実施例構成図



【図10】

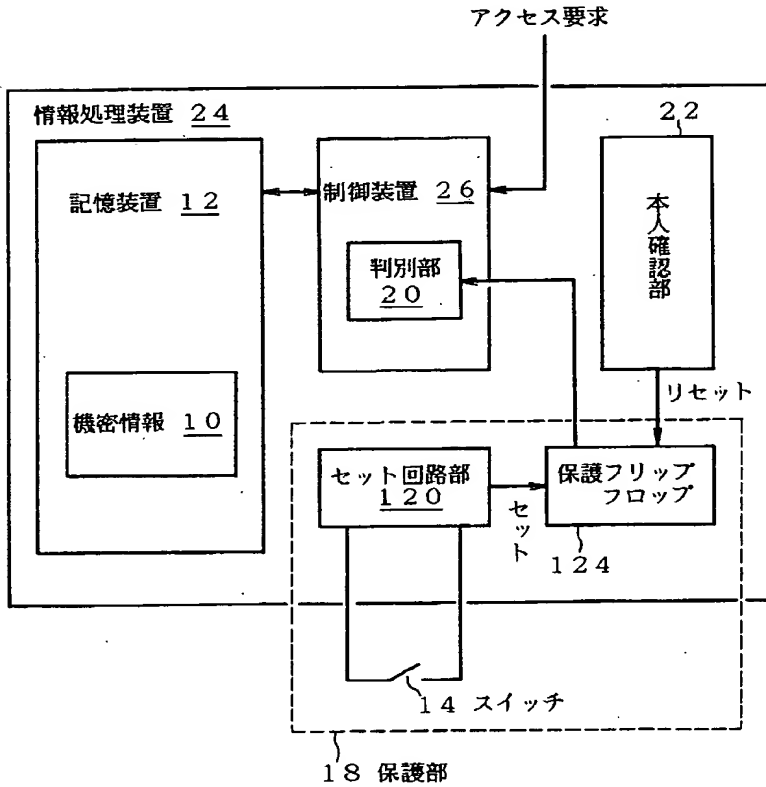
監視部により監視情報の消去条件を判別するようにした計算機本体の他の実施例

構成図



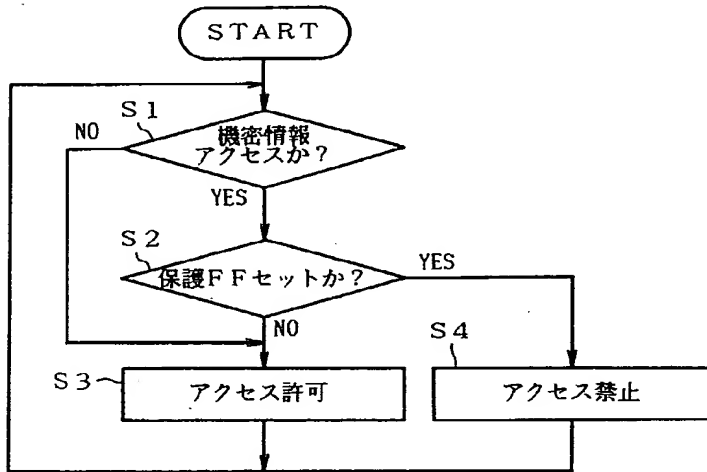
【図11】

本発明の基本的な第2実施例を示した実施例構成図



【図12】

図10の実施例による機密情報の保護処理を示したフローチャート



【図13】

図11の実施例を適用したマイクロコンピュータ計算機本体の実施例構成図

